

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-247949

(43)Date of publication of application : 14.09.1998

(51)Int.Cl. H04L 12/66
 G09C 1/00
 H04L 9/32
 H04M 3/00
 H04M 11/00
 H04N 1/00
 H04N 1/32
 H04N 1/44

(21)Application number : 09-050137

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 05.03.1997

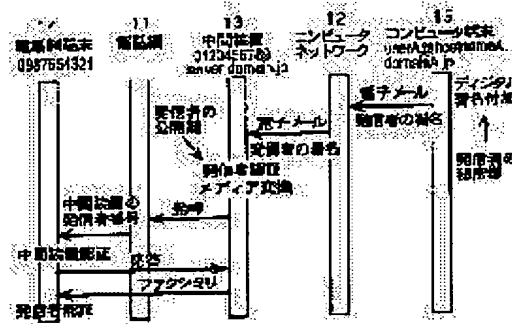
(72)Inventor : YAMADA TOMOHIRO
TAKAHASHI ISAMU
SUZUKI AKIRA

(54) CALLER AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To surely authenticate a caller in the case of communication between a telephone network terminal 14 and a computer terminal 15 via an intermediate device 13.

SOLUTION: A terminal 15 gives a digital signature to a message by using its private key and send the resulting message to an intermediate device 13, and the device 13 authenticates the signature by using a public key and when the signature passes the authentication, the device 13 converts the message into FAX image data and send the data to a terminal 14, the terminal 14 compares the caller number with a caller number of the device 13 stored in advance and receives the FAX data when they are coincident and the terminal 14 authenticates the caller of the terminal 15 from the reproduced image.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(11)特許出願公開番号

(43)公開日 平成10年(1998)9月14日

(51)Int.Cl. ⁶	識別記号	F I	
H 0 4 L 12/66		H 0 4 L 11/20	B
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
H 0 4 L 9/32		H 0 4 M 3/00	B
H 0 4 M 3/00		11/00	3 0 3
11/00	3 0 3	H 0 4 N 1/00	1 0 7 A

審査請求 未請求 請求項の数 7 O L (全 13 頁) 最終頁に続く

(21)出願番号	特願平9-50137	(71)出願人	000004226 日本電信電話株式会社 東京都新宿区西新宿三丁目19番2号
(22)出願日	平成9年(1997)3月5日	(72)発明者	山田 智広 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(72)発明者	高橋 勇 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(72)発明者	鈴木 晃 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(74)代理人	弁理士 草野 卓

(54) 【発明の名称】 発信者認証方法

(57) 【要約】

【課題】 電話網端末 14 とコンピュータ端末 15 とが中間装置 13 を介して通信する際に発信者認証を確実に
行う。

【解決手段】 端末１５はメッセージにその秘密鍵によるデジタル署名を付けて中間装置１３へ送信し、装置１３は端末１５の公開鍵で署名を検証し合格すると、メッセージをＦＡＸ画像データに変換して端末１４へ送り、端末１４は発信者番号を予め記憶した装置１３の発信者番号と比較し、一致すればＦＡＸを受信し、その再生画像から端末１５の発信者認証を行う。

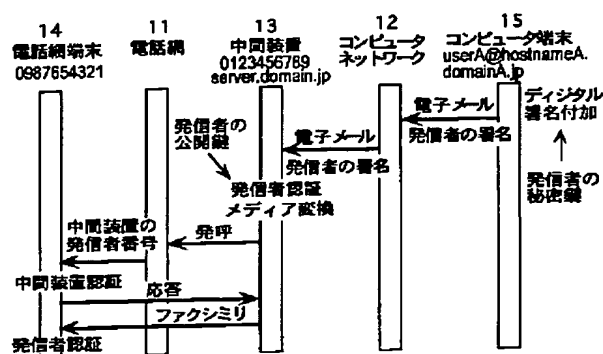


图 6

【特許請求の範囲】

【請求項 1】 電話網に收容された電話網端末と、コンピュータネットワークに收容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記コンピュータ端末からメッセージを発信する際に、そのメッセージにそのコンピュータ端末を使用する発信者のデジタル署名を付けて送信し、

上記中間装置で受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項 2】 上記中間装置の発信者番号を上記電話網端末に記憶しておき、

上記電話網端末は上記中間装置から通信要求があると、その発信者番号を上記記憶した発信者番号とを照合して中間装置の認証を行うことを特徴とする請求項 1 記載の発信者認証方法。

【請求項 3】 上記電話網端末は、上記発信者番号の照合が合格すると、上記中間装置からメッセージと共に通知された上記コンピュータ端末の発信者情報により発信者の認証を行うことを特徴とする請求項 2 記載の発信者認証方法。

【請求項 4】 上記中間装置に受信したメッセージのメッセージ ID を記憶し、

上記コンピュータ端末はその送信メッセージにメッセージ ID を与え、このメッセージ ID に対しても上記デジタル署名を行い、

上記中間装置は上記コンピュータ端末からのメッセージ中のメッセージ ID をそれ以前記憶した上記メッセージ ID と比較し、一致すると、不正メッセージとして処理することを特徴とする請求項 1 乃至 3 の何れかに記載の発信者認証方法。

【請求項 5】 電話網に收容された電話網端末と、コンピュータネットワークに收容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記中間装置は上記電話網端末より受信したメッセージを、これに対し中間装置のデジタル署名を付けて上記コンピュータ端末へ送信し、

上記コンピュータ端末は受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項 6】 上記電話網端末の発信者番号を上記中間装置に記憶しておき、

上記中間装置は上記電話網端末からの通信要求があると、その発信者番号を上記記憶した発信者番号と照合して発信者の認証を行うことを特徴とする請求項 5 記載の発信者認証方法。

【請求項 7】 上記メッセージの署名の認証に合格すると、上記中間装置からメッセージと共に通知された上記電話網端末の発信者情報により発信者の認証を行うことを特徴とする請求項 5 又は 6 記載の発信者認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コンピュータネットワークと電話網の端末間で相互にメッセージ通信を行う通信における発信者の認証方法に関するものである。

【0002】

【従来の技術】図 12 に示すように公衆電話網 11 とコンピュータネットワーク 12 とのそれぞれにインタフェースをもつ中間装置（以下単に中間装置と記す）13 が設けられ、電話網 11 に收容された電話網端末 14 とコンピュータネットワーク 12 に收容されたコンピュータ端末 15 とが中間装置 13 を介してメッセージを通信する通信方法が知られている。

【0003】従来、このようなコンピュータネットワーク 12 と電話網 11 の端末 15、14 間で相互にメッセージ通信を行うサービスでは、課金等のための発信者認証を行う方法として、目的に応じて主に次の 2 つの方法が取られている。第 1 の方法は、予め中間装置 13 に電子メールアドレスを登録し、コンピュータネットワーク 12 側からの電子メールを中間装置 13 を経由して電話網端末としてのファクシミリ端末 14 へ送信する場合は、図 1 に示すように、発信コンピュータ端末 15 から中間装置 13 に電子メールが送られて来ると、中間装置 13 は電子メール内の発信端末 15 のメールアドレスを予め登録した電子メールアドレスと照合することにより発信者認証を行い、その認証に合格すればコンピュータ端末 15 より受信した電子メール内のテキスト（文字）や画像などのメッセージをファクシミリ信号に変換し、つまりメディア変換を行って着信側へ電話網のファクシミリ端末 14 へ送信する。中間装置 13 を介してファクシミリ端末 14 に着信があると、ファクシミリ端末 14 の受信者はファクシミリ端末 14 の再生画像中のメッセージに添付されている前記電子メールアドレスにより発信者の確認を行う。

【0004】また、電話網端末 14 側からファクシミリをコンピュータ端末 15 に送信する場合は図 2 に示すように中間装置 13 においては、端末 14 から受信したファクシミリに対しては特に発信者認証を行わず、そのファクシミリ信号を電子メールの形式にメディア変換して着信側のコンピュータ端末 15 へ送信する。この電子メールを受信したコンピュータ端末 15 の受信者は端末 14 の発信者が付加したカバーページにより発信者の確認を行う。

【0005】第 2 の方法は、予め中間装置 13 に発信者を認証するための ID（利用者識別情報）とパスワード

を登録し、コンピュータネットワーク12側からの電子メールを中間装置13を経由して電話網11のファクシミリ端末14に送信する場合は、図3に示すように、発信コンピュータ端末15で発信者を認証するためのIDとパスワードを電子メールに添付して、中間装置13に対して電子メールを送信し、中間装置13は受信した電子メール内のIDとパスワードを予め登録したIDとパスワードと照合することにより発信者認証を行い、認証に合格すればその電子メールのメッセージをファクシミリ信号に変換して電話網のファクシミリ端末14に送信する。ファクシミリ端末14の受信者はファクシミリ端末14の再生画像メッセージに付加されている発信者のIDにより発信者の確認を行う。

【0006】また、電話網11側からファクシミリをコンピュータ端末15へ送信する場合は、図4に示すように、発信者がPB音で発信者を認証するためのIDとパスワードをファクシミリ端末14より入力し、中間装置13はその入力されたIDとパスワードを予め登録したIDとパスワードと照合することにより発信者認証を行い、これに合格するとその後送られて来たファクシミリを電子メールに変換してコンピュータ端末15へ送信する。コンピュータ端末15の受信者は受信した電子メールのメッセージに付加されている発信者IDにより発信者の確認を行う。

【0007】

【発明が解決しようとする課題】従来の第1の方法では、発信者の電子メールアドレスが漏洩した場合、第3者が不正に発信者の電子メールアドレスを偽装してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第3者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網11からファクシミリをコンピュータ端末へ送信する際には中間装置13で認証を行わないため、第3者が不正にファクシミリを送信することにより、中間装置13の管理者に不利益をもたらすおそれがあり、また、発信者が特定できないメッセージが受信者に送信されることにより、受信者の不利益になるおそれがあるという問題点があった。

【0008】従来の第2の方法では、従来の第1の方法と同様に、第3者が不正に発信者のIDとパスワードを偽装しメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第3者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網11からファクシミリをコンピュータ端末15へ追信する際にも、第3者が不正に発信者のIDとパスワードを偽装使用してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合があるという問題点があった。

【0009】この発明は、第3者が発信者になりすまし、あるいは第3者がメッセージを改ざんすることにより発信者および受信者の不利益になるという問題点および第3者が不正にファクシミリを送信することにより中間装置の管理者の不利益になるという問題点を解決した、発信者認証方法を提案することを目的とする。

【0010】

【課題を解決するための手段】この発明は、コンピュータ端末より発信する場合はデジタル署名を行い、中間装置でメッセージに付加されたデジタル署名を使用して発信者認証を行うことで、第3者によるなりすましの防止およびメッセージに対する改ざんの検出を可能とし、電話網端末よりの発信に対しては電話網より通知される発信者番号を使用して発信者認証を行うことで、第3者によるなりすましの防止を可能とし、電話網端末に着信があると、その受信者は中間装置13より通知される中間装置の発信者番号および受信メッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認を可能とし、コンピュータ端末に着信があるとその受信者は受信メッセージに付加された中間装置のデジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発信者の確認を可能とする。

【0011】

【作用】中間装置での認証において、コンピュータネットワークに接続されている発信者に対しては、メッセージに付加されたデジタル署名を使用して発信者認証を行うことで、第3者が発信者の電子メールアドレスを偽ったとしても、デジタル署名が異なれば、不正なメッセージとして破棄することができるとなる。また、デジタル署名は発信者のみが作成できかつメッセージ毎に異なる為、第3者が不正にデジタル署名を複製した場合およびメッセージの一部が改ざんされた場合であっても検出することが可能になる。また、電子メール装置により一意に付与されるメッセージIDに対してもデジタル署名を施すことにより、同一のメッセージIDを持つメッセージを破棄することで、メッセージ全体を不正に複製した場合であっても検出が可能となる。電話網に接続されている発信者に対しては、発信者からではなく、電話網より通知される発信者番号を使用して発信者認証を行うことで、第3者が不正に成りすますことを防ぐことが可能になる。受信者での認証においても、電話網に接続されている受信者は、予め中間装置の発信者番号のみを取得しておくことで、電話網より通知される中間装置の発信者番号およびメッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認が可能となり、コンピュータネットワークに接続されている受信者は、予め中間装置の公開鍵のみを取得しておくことで、中間装置のデジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発

信者の確認が可能となる。

【0012】

【発明の実施の形態】

実施例 1

図 1 A にこの発明が適用される通信システムの一例を示し、図 1 2 と対応する部分に同一符号を付けてある。電話網 1 1 は発信者番号通知手段 2 1 を備えているものである。電話網端末 1 4 は電話網 1 1 との信号の送受を行う通信制御手段 2 2 を備え、またこの例ではファクシミリ端末の場合であり、画像入出力手段 2 3 を備え、この発明では更に、受信メッセージから発信者番号抽出手段 2 4、更に中間装置 1 3 の発信者番号を記憶する蓄積手段 2 5 を備えている。

【0013】中間装置 1 3 は電話網 1 1、コンピュータネットワーク 1 2 とそれぞれ通信の送受を行う通信制御手段（インタフェース）2 6、2 7 を備えている他に、この発明では、発信者番号抽出手段 2 8、送信メッセージにデジタル署名を付加する手段 2 9、メディア変換手段 3 0、受信デジタル署名を照合（検証）する手段 3 1、更に、デジタル署名、とその検証に必要な公開鍵、秘密鍵を記憶する蓄積手段 3 2 を備えている。

【0014】コンピュータ端末 1 5 はコンピュータネットワーク 1 2 との通信の送受を行う通信制御手段 3 3、電子メールの入出力手段 3 4 を備えている他に、この発明では送信メッセージにデジタル署名を付加する手段 3 5、受信デジタル署名を照合（検証）する手段 3 6、デジタル署名、その検証に必要な公開鍵、秘密鍵を記憶する蓄積手段 3 7 を備えている。

【0015】この発明ではデジタル署名を利用するが、これに必要な鍵の取得について、図 2 を参照して説明する。中間装置 1 3 は公開鍵と秘密鍵の対を生成して、公開鍵を、認証局 3 9 に登録すると共に秘密鍵を蓄積手段 3 2 に記憶する。コンピュータ端末 1 5 は認証局 3 9 から中間装置 1 3 の公開鍵を取得し、また公開鍵と秘密鍵の対を生成し、その公開鍵を認証局 3 9 に登録すると共に秘密鍵を蓄積手段 3 7 に記憶し、更に自己の名前などの利用者情報（ID）に対し、コンピュータ端末 1 5 の秘密鍵でデジタル署名を添付して、これを中間装置 1 3 の公開鍵で暗号化して中間装置 1 3 へ送信する。中間装置 1 3 はその受信データを中間装置 1 3 の秘密鍵で復号化し、また、認証局 3 9 からコンピュータ端末 1 5 の公開鍵を取得し、この公開鍵で前記復号化デジタル署名を検証し、合格すれば、その受信した復号化したコンピュータ端末 1 5 の利用者情報を蓄積手段 3 2 に蓄積登録し、その登録結果を示すメッセージを作成して、これに対し中間装置 1 3 の秘密鍵で署名し、その署名付登録結果メッセージをコンピュータ端末 1 5 の公開鍵で暗号化してコンピュータ端末 1 5 へ送信する。コンピュータ端末 1 5 は受信した暗号化データを秘密鍵で復号化し、その復号化された署名を中間装置 1 3 の公開鍵

で検証し、その登録内容を確認する。

【0016】この実施例 1 はコンピュータ端末 1 5 から、中間装置 1 3 を経由して、電話網端末 1 4 に対してメッセージを送信する場合である。この場合電子メール装置（コンピュータ端末）1 5 を使用する発信者は予め、例えば図 2 で説明した方法により、認証に必要な情報である発信者（コンピュータ端末 1 5）の加入者情報を中間装置 1 3 内の加入者情報蓄積手段 3 2 に登録しておき、中間装置 1 3 は発信者の認証に必要なコンピュータ端末 1 5 の公開鍵を取得し、加入者情報蓄積手段 3 2 に記憶しておく、また、電話網端末 1 4、この実施例ではファクシミリ端末を使用する受信者は予め、中間装置 1 3 の認証に必要な中間装置 1 3 の発信者番号を情報蓄積手段 2 2 に蓄積しておく。

【0017】コンピュータ端末 1 5 からメッセージを送信する際に、メール入出力手段 3 4 によりメッセージを作成し、デジタル署名付加手段 3 5 により、前記作成したメッセージに対して、コンピュータ端末 1 5 の秘密鍵を使用し、発信者のデジタル署名を付加する。このデジタル署名を付加したメッセージは、通信制御手段 3 3 により、中間装置 1 3 に対して送信される。

【0018】中間装置 1 3 はこのメッセージを通信制御手段 2 7 より受信し、デジタル署名照合手段 3 1 により、予め蓄積手段 3 2 に蓄積されたコンピュータ端末 1 5 の公開鍵を使用して、メッセージに付加されたデジタル署名の照合を行う。照合を行った結果、デジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、メディア変換手段 3 0 により、電子メールの内容をファクシミリ画像に変換する。デジタル署名が不正であった場合はメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段 2 6 により、電話網端末 1 4 に対して送信される。中間装置 1 3 から電話網端末 1 4 に対する発呼があると、電話網 1 1 は発信者情報通知手段 2 1 により、中間装置 1 3 の発信者番号を受信端末 1 4 に通知する。受信端末 1 4 は発信者番号抽出手段 2 4 により発信者番号を抽出し、情報蓄積手段 2 5 に蓄積されている中間装置 1 3 の発信者番号により、中間装置 1 3 からの着呼であることを確認したのち、通信制御手段 2 2 によりファクシミリの受信を行う。受信したファクシミリの再生画像は発信者の情報が付加されている為、発信者が中間装置 1 3 に登録されている発信者であることが確認できる。

【0019】なお、コンピュータ端末 1 5 で作成する電子メールは例えば図 3 に示すようなものである。即ち、まず発信者アドレス 6 1 が記述され、次に以下の記述のフォーマット 6 2（この例では MIME バージョン 1.0）が示され、これに相手先（受信者）アドレス 6 3 が続き、更に主題 6 4 がこの例では日本語 J I S コードでテストであることが記述され、次に内容形式 6 5 がこの

例ではマルチパート／混合で境界を“・・・742959F6218E”で示し、この境界66を付けて、内容形式67がこの例ではテキスト／通常、文字はJIS規格コードであることが示され、更に内容変換符号化68がこの例では7ビット符号であることが示された後にメッセージ内容であるテキスト69が記述される。次の境界70の後に内容形式71がこの例では画像であり、そのフォーマットがgifであることが示され、その内容変換符号化72がこの例ではbase64によることが示され、次にその符号化された画像データ73が記述され、その終りに境界74が付けられる。

【0020】このメッセージに対し署名した電子メールは例えば図4に示すようになる。つまり発信アドレス61、記述フォーマット62、着信アドレス63、主題64は図3と同一であり、次の内容形式65で、マルチパート、署名付きとなり、かつ境界が“Next Part Level-1-152633”となり、署名アルゴリズムがpgpmd5であることが記述され、境界66の次の内容形式67でメッセージであることとそのフォーマットrfc822が記述された後に、図3中の全メッセージの記述75がなされ、その終りの境界76に続く内容形式77にpgp法による署名であり、その署名データ78が続き、最後に境界79が付けられている。

【0021】中間装置13内のメディア変換手段30では、この例では受信メッセージ中のテキスト（文字）69が例えば図5に示すようにファクシミリ画像のデータに変換され、また画像メッセージ73も図5に示すようにファクシミリ画像のデータに変換される。この場合、両画面の左上端部に発信者アドレスと主題とが画像データとして付け加えられる。

【0022】上述した実施例の処理の流れを図6に示す。コンピュータ端末15では作成したメッセージに対し、端末15の秘密鍵で署名し、この署名付きメッセージを電子メールとして中間装置13へ送る。中間装置13は端末15の公開鍵で署名を検証し、合格すれば、そのメッセージをメディア変換して電話網端末（ファクシミリ端末）14を呼出し、端末14は中間装置13の発信者番号を確認し、正しければ、中間装置13に応答し、ファクシミリを受信する。そのファクシミリの再生画像中の発信アドレスから、その発信者、つまりコンピュータ端末15から発信されたものであることを確認する。

実施例2

図7にこの発明の実施例を示す。これは電話網端末14から中間装置13を経由して、コンピュータ端末15にメッセージを送信する場合である。

【0023】電話網端末としてのファクシミリ端末14を使用する発信者は予め、認証に必要な自分の発信者番号を中間装置13内の加入者情報蓄積手段32に登録を

行う。また、コンピュータ端末の電子メール装置15を使用する受信者は、中間装置13の認証に必要な中間装置の公開鍵を認証局から取得し、情報蓄積手段37に蓄積しておく。ファクシミリ端末14からコンピュータ端末15へメッセージを送信する際に、ファクシミリ入出力手段23により例えば図8に示すようなファクシミリ画像を入力する。入力されたファクシミリ画像は、通信制御手段22により、中間装置13に対して送信される。その際に端末14から中間装置13に対して発呼があると、電話網11は発信者情報通知手段21により、発信端末14の発信者番号を中間装置13に通知する。中間装置13は、発信者番号抽出手段28により、発信端末の発信者番号を抽出した後、加入者情報蓄積手段32に蓄積されている端末14の発信者番号と照合する。照合した結果が正しい場合は通信制御手段26により、ファクシミリの受信を行う。発信者番号が一致しない場合は不正な着呼と判断し、受信を行わない。受信したファクシミリ画像は、メディア変換手段30により例えば図9に示すような電子メールのフォーマットに変換する。この電子メールは図3の場合と同様に、発信アドレス61、記述フォーマット62、受信アドレス63、主題64（この例ではFAX）であり、内容形式65が記述された後の境界66の次は図3中の画像メッセージ部分と対応したものが続く。

【0024】この電子メールフォーマットに変換されたメッセージは、デジタル署名付加手段29により、図4に示した場合と同様に中間装置13のデジタル署名を付加する。デジタル署名を付加したメッセージは、通信制御手段27によりコンピュータ端末（電子メール装置）15に送信される。コンピュータ端末15は通信制御手段33により、メッセージを受信した後、デジタル署名照合手段36により、情報蓄積手段37に予め取得した中間装置13の公開鍵を使用して、メッセージに付加されたデジタル署名の照合を行う。照合した結果が正しければ、その電子メール中のFrom行に記載されている発信者情報（アドレス）により、発信者が中間装置13に登録されている発信者であることが確認できる。

実施例3

この実施例は、コンピュータ端末15から中間装置13を経由して、電話網端末14に対してメッセージを送信する場合で、実施例1との違いは、発信者が作成したメッセージにのみデジタル署名を施すのではなく、コンピュータ端末15内の通信制御手段33により付加されるメッセージIDに対してもデジタル署名を施し、これにより、メッセージIDが改ざんされることがなくなり、メッセージIDにより、一意にメッセージの識別を行うことを可能とする。これを実現するため、中間装置13内に受信したメッセージIDを記憶するID蓄積手段41が図1に実線で示すように設ける。

【0025】この処理手順を図10に示す。実施例と同様にコンピュータ端末15の公開鍵を中間装置13に登録し、また中間装置13の発信者番号を電話網端末14の情報蓄積手段25に蓄積しておく。コンピュータ端末15からメッセージを送信する際に、入出力手段34によりメッセージを作成し、このメッセージに対して通信制御手段33により、メッセージIDを付加する。デジタル署名付加手段35により、前記メッセージに対して、自分のデジタル署名を付加して通信制御手段33により、中間装置13に対して送信する。

【0026】メッセージを受信した中間装置13は、デジタル署名照合手段31により、予め蓄積手段32に蓄積された利用者情報を使用して、メッセージに付加されたデジタル署名の照合を行う。デジタル署名が不正であった場合はメッセージを破棄する。照合を行った結果、デジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、次にID蓄積手段41に蓄積されている全てのメッセージIDと受信メッセージ中のメッセージIDとの比較を行う。メッセージIDが異なる場合は、メッセージ中のメッセージIDをID蓄積手段41に蓄積し、メディア変換手段30により、電子メールの内容を図5に示したようなファクシミリ画像のデータに変換する。前記メッセージIDの比較の結果、そのメッセージIDがすでに、メッセージID蓄積手段41に存在する場合は、この受信メッセージは不正に複製されたものと判断し、そのメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段26により、電話網端末14とのファクシミリ端末へ送信する。この後の処理は実施例1と同様である。

【0027】公開鍵の取得方法としては例えば図11に示すように行ってもよい。図2の場合と同様に中間装置13、コンピュータ端末15はそれぞれ公開鍵と秘密鍵の対を生成し、公開鍵と自分の情報とをそれぞれ認証局39に登録を行う。その際に登録内の確認証明書を認証局39から発行してもらい、その証明書を蓄積手段32、37にそれぞれ蓄積しておく。コンピュータ端末15はその利用者情報を中間装置13に登録するために、まず中間装置13から中間装置の証明書を取得し、また認証局39から認証局39の公開鍵を取得し、この公開鍵を用いて、取得した中間装置の証明書の認証を行い、その認証に合格すれば、その証明書から、中間装置13の公開鍵を取出し、その公開鍵でコンピュータ端末15の利用者情報を暗号化し、これに対するコンピュータ端末15の秘密情報で署名を行い、その署名付き暗号化利用者情報と、コンピュータ端末の証明書を中間装置13へ送信する。

【0028】中間装置13では、認証局39から認証局の公開鍵を受取り、この公開鍵で受信したコンピュータ端末の証明書を認証し、これに合格すれば、その証明書

からコンピュータ端末15の公開鍵を取出し、その公開鍵を蓄積手段32に蓄積すると共にその公開鍵で受信した暗号化利用者情報の署名を検証し、これに合格すれば、その暗号化利用者情報を中間装置13の秘密鍵で復号化し、その利用者情報の内容に間違いがないかを確認した後、利用者情報を蓄積手段32に記憶する。その登録結果メッセージをコンピュータ端末15の公開鍵で暗号化し、その暗号化登録結果を、これに対し中間装置13の署名を付け、更に中間装置の証明書も付けてコンピュータ端末15へ送る。

【0029】コンピュータ端末15は同様にして、受信登録結果の署名を中間装置の公開鍵で検証し、更に、コンピュータ端末15の秘密鍵で復号化して登録内容を確認する。このように証明書を発行してもらい、コンピュータ端末15（あるいは中間装置13）から送信するメッセージにそのコンピュータ端末15（中間装置13）の証明書を付けて送信すれば、受信した中間装置13（コンピュータ端末15）は受信した証明書からコンピュータ端末15（中間装置13）の公開鍵を得ることができる。従って中間装置13は認証局39からコンピュータ端末15の公開鍵を取得する必要はない。

【0030】

【発明の効果】以上説明したように、請求項1乃至4の発明によれば、コンピュータ端末15からのメッセージの受け付けにおいて、中間装置13で第3者によるなりすましの防止およびメッセージに対する改ざんの検出が可能となり、また、第3者によるメッセージの複製を検出することが可能となり、発信者への課金が正しく行われるという経済的効果がある。

【0031】また、請求項5乃至7の発明によれば、電話網端末14からのメッセージの受け付けにおいて、中間装置13で第3者によるなりすましの防止が可能となり、発信者への課金が正しく行われるという経済的効果がある。また、請求項2の発明によれば、受信端末における発信者認証において、予め中間装置の情報を取得しておくだけで、発信者が正しいか否かの確認が可能になるというサービス性を向上させる効果がある。

【図面の簡単な説明】

【図1】この発明方法が適用される通信システムの例を示すブロック図。

【図2】この発明に用いられる公開鍵取得方法の手順を示す図。

【図3】コンピュータ端末15で作られたメッセージの例を示す図。

【図4】コンピュータ端末15で図3のメッセージをデジタル署名した電子メールの例を示す図。

【図5】図3のメッセージをファクシミリ画像に変換した例を示す図。

【図6】請求項2の発明の実施例のシーケンスを示す図。

【図7】請求項5の発明の実施例のシーケンスを示す図。

【図8】送信ファクシミリ画像の例を示す図。

【図9】図8のファクシミリ画像を電子メッセージに変換した例を示す図。

【図10】請求項4の発明の実施例のシーケンスを示す図。

【図11】公開鍵取得の他の方法のシーケンスを示す図。

【図12】この発明方法が適用される通信システムの例 10

を示す図。

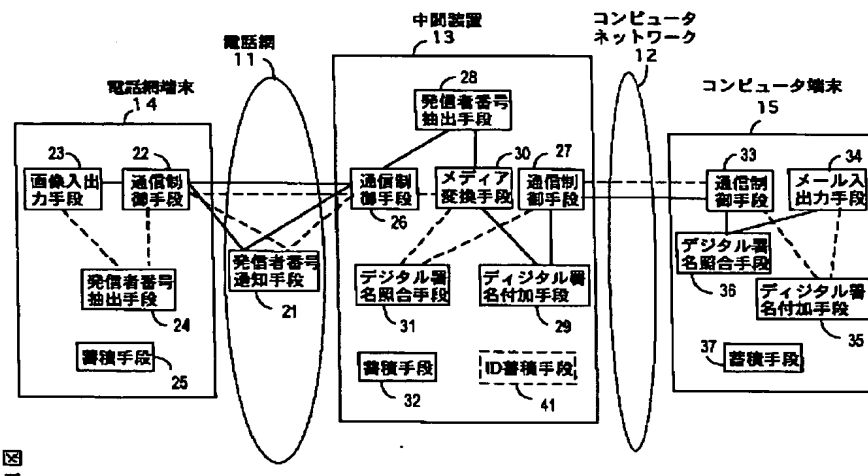
【図13】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図14】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図15】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図16】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図1】



図

【図6】

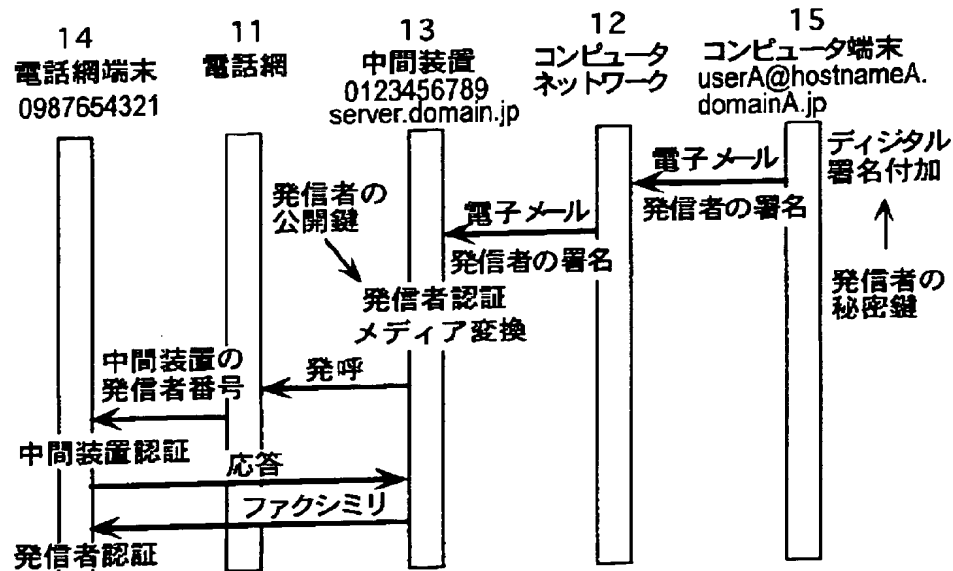


図6

【図2】

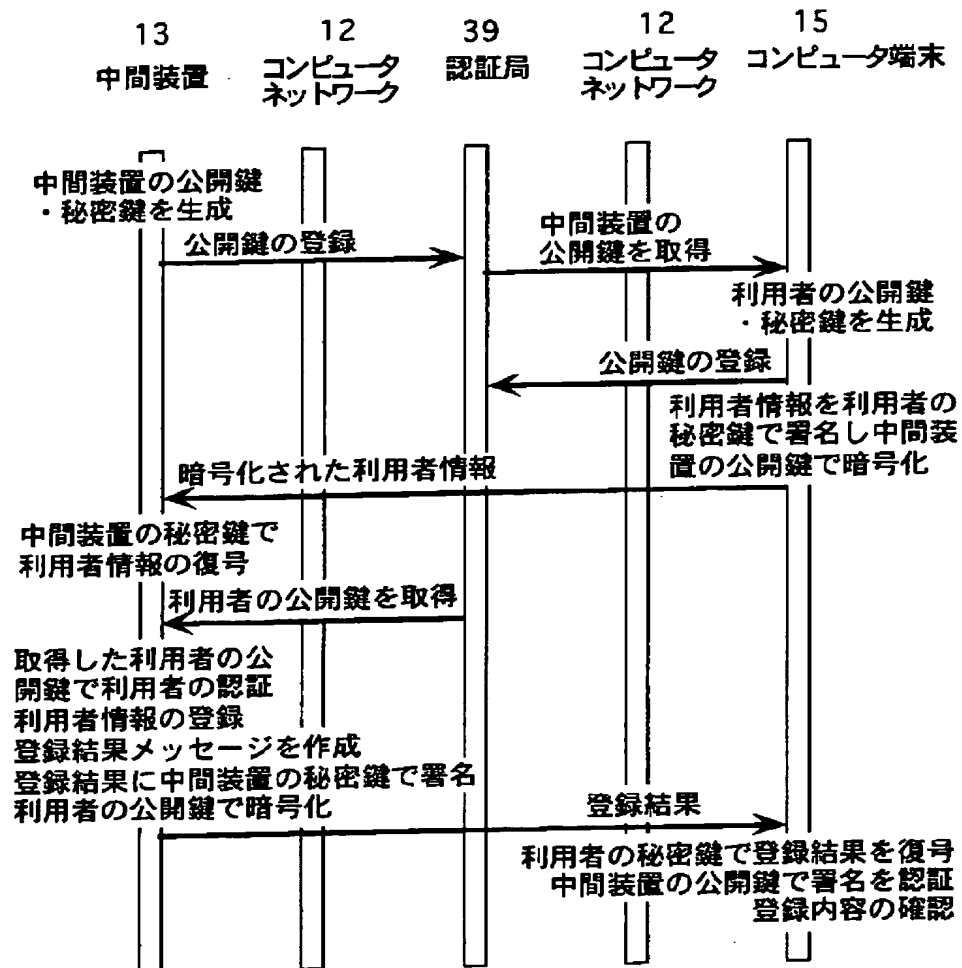


図 2

【図12】



図12

【図3】

```

61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYIOSVIGyhK?=?
65 Content-Type: multipart/mixed; boundary=".....742959F6218E"

This is a multi-part message in MIME format.

66 .....742959F6218E
67 Content-Type: text/plain; charset=iso-2022-jp
68 Content-Transfer-Encoding: 7bit

69 こんにちは。
   これはテストです。

70 .....742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

{
  R0lGODlhawBaAPcAAP///Hu7Ofb0vPqsDAwMXFwG0k8uili
  KWlpYWVhXlpZfpaWkA/PjAwMBYVfQAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  <中略>
73 mDXSW8oSTgCv5yOIPMZVzKld9AJFFgWabTLXa57EPiWpURv
  R2PhVzdCtDzIZHB7PeFg79CfG3mxUfEs4wPcnIZxfQd+hy7
  byAkHXoUhdFKtKDD33JerRZU8epthWdykU4Lhryt6U56vIFg/
  kMVPFFczHMSaCDKC+MIRBYgbgRUGQXAD2QbCs92sBSzbpVm
  Mi07230gs8kqIQ+ajzJgkBEEx+0ABjLkYwb98jHPvnxj4C8TUA
  AADs=
74 .....742959F6218E.....

```

図 3

【図4】

```

61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYIOSVIGyhK?=?
65 Content-Type: multipart/mixed; boundary="Next_Part_Level_1_152633";
   micalg=pgpmd5;
   protocol="application/pgp-signature"

66 ....Next_Part_Level_1_152633
67 Content-Type: message/rfc822

From: userA@hostnameA.domainA.jp
MIME-Version: 1.0
To: 0987654321@server.domain.jp
Subject: =?iso-2022-jp?B?GyRCJUYIOSVIGyhK?=?
Content-Type: multipart/mixed; boundary=".....742959F6218E"

This is a multi-part message in MIME format.

.....742959F6218E
Content-Type: text/plain; charset=iso-2022-jp
Content-Transfer-Encoding: 7bit

75 こんにちは。
   これはテストです。

.....742959F6218E
Content-Type: image/gif; name="textimage1.gif"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="textimage1.gif"

R0lGODlhawBaAPcAAP///Hu7Ofb0vPqsDAwMXFwG0k8uiliKWlpYWVhXlpZ
FpaWkA/PjAwMBYVfQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
<中略>
IFgAMVPFFczHMSaCDKC+MIRBYgbgRUGQXAD2QbCs92sBSzbpVmM072
30gs8kqIQ+ajzJgkBEEx+0ABjLkYwb98jHPvnxj4C8TUAADs=
.....742959F6218E.....

76 ....Next_Part_Level_1_1512633
77 Content-Type: application/pgp-signature

.....BEGIN PGP SIGNATURE.....
Version: 2.6.2
78 IQBVAwUBMvWlWu8FMT+s8kpaQFUCAHMOXF1AkhNPzaylthD3icowr59z
n5KmCz+MvWnCZlnZYEEY4mq8igDc3jwemXnfQZ3TEYtGNuHYRTZbg=
=9Qb6
79 .....END PGP SIGNATURE.....

.....Next_Part_Level_1_152633-

```

図 4

【図5】

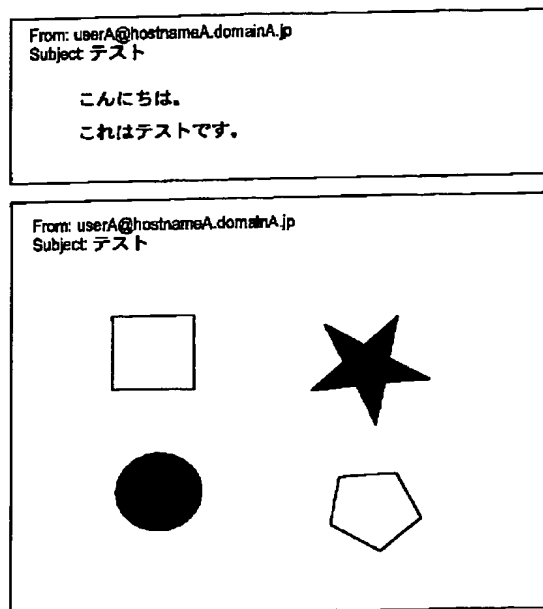


図 5

【図8】

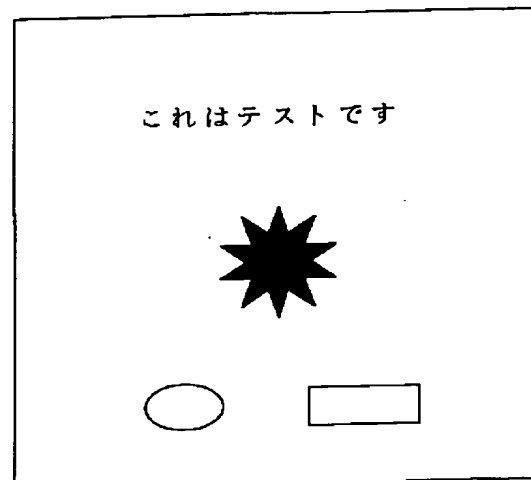


図 8

【図7】

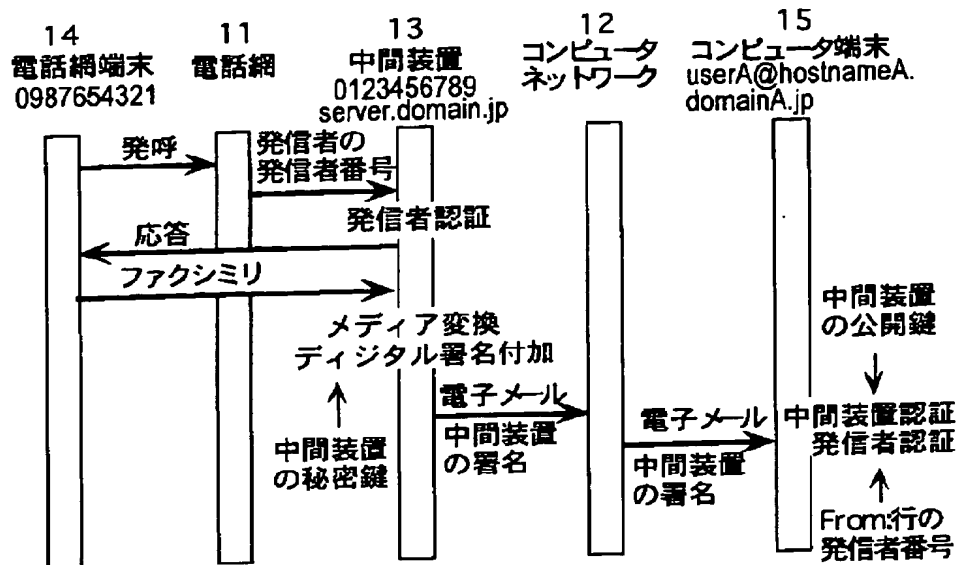


図7

【図9】

```

61 From: 0987654321@server.domainA.jp
62 MIME-Version: 1.0
63 To: userA@hostnameA.domain.jp
64 Subject: FAX
65 Content-Type: multipart/mixed; boundary=".....742959F6218E"

68 .....742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

73 <中略>
9mRRNmXnYoiVGvd9mVhVl9NWZptmZ9mZdNmd1dmd5md99
meBNqRohXZaibZofZokTZp1XZpmbZpnfZpoTZapXZqpbZqfZqs
TZrXZrubZrnfZrwTZsXZsybZszfZs0TZ1XZ12bZ13Z14TZu5XZu6b
Zu7TZu8TZv9XZv++bZvTZvATdwBXdwCbdwDfdwETdxFXdxGbdxExf
dxITdyJXdyKbdyLfdyMTdzNXdxObdzPfdzQTd0RXdx0Sbd0Tfd0UTd
1VXdIg6AAAAA7
74 .....742959F6218E....

```

図9

【図13】

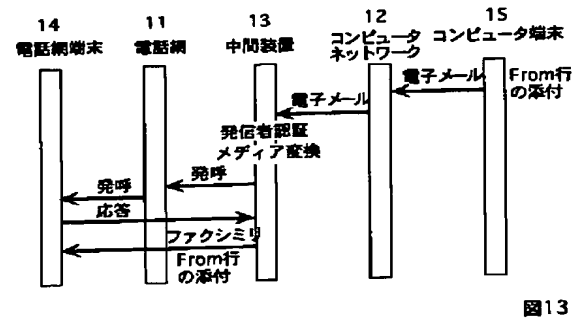


図13

【図14】

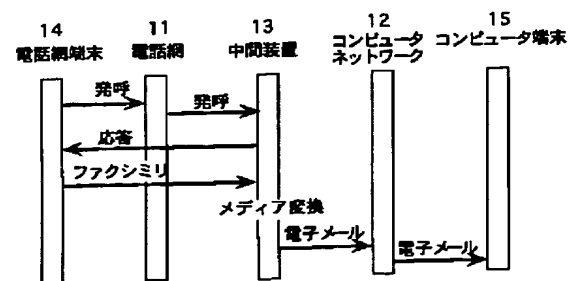
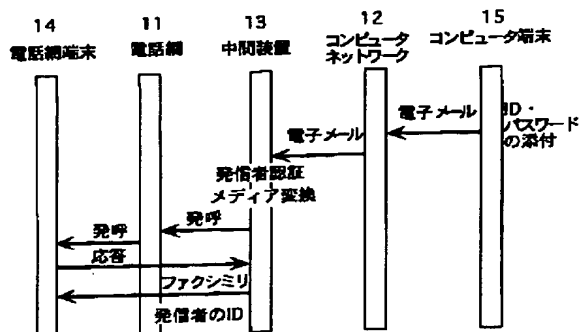


図14

The diagram illustrates a fax transmission process involving four entities: 14 電話網端末 (Telephone Network Terminal), 11 電話網 (Telephone Network), 13 中間装置 (Intermediate Device), 12 コンピュータネットワーク (Computer Network), and 15 コンピュータ端末 (Computer Terminal). The process is as follows:

- 14 電話網端末** (0987654321) sends a **発呼** (Call) to **11 電話網**.
- 11 電話網** sends a **応答** (Response) to **14 電話網端末**.
- 11 電話網** sends **中間装置の発信者番号** (Intermediate Device's Caller Number) to **13 中間装置**.
- 13 中間装置** (0123456789, server.domain.jp) sends **発信者の公開鍵** (Sender's Public Key) to **12 コンピュータネットワーク**.
- 12 コンピュータネットワーク** sends **電子メール** (Email) and **発信者の署名** (Sender's Signature) to **13 中間装置**.
- 13 中間装置** performs **発信者認証** (Sender Authentication), **メッセージIDの蓄積** (Message ID Storage), and **メディア変換** (Media Conversion).
- 13 中間装置** sends **電子メール** and **発信者の署名** to **15 コンピュータ端末** (userA@hostnameA.domainA.jp).
- 15 コンピュータ端末** sends **デジタル署名付加** (Digital Signature Addition) to **13 中間装置**.
- 15 コンピュータ端末** sends **発信者の秘密鍵** (Sender's Secret Key) to **13 中間装置**.
- 13 中間装置** sends **中間装置認証** (Intermediate Device Authentication) to **14 電話網端末**.
- 14 電話網端末** sends **発信者認証** (Sender Authentication) to **13 中間装置**.
- 13 中間装置** sends **ファクシミリ** (Facsimile) to **14 電話網端末**.

【图 16】



- 11 -

【図11】

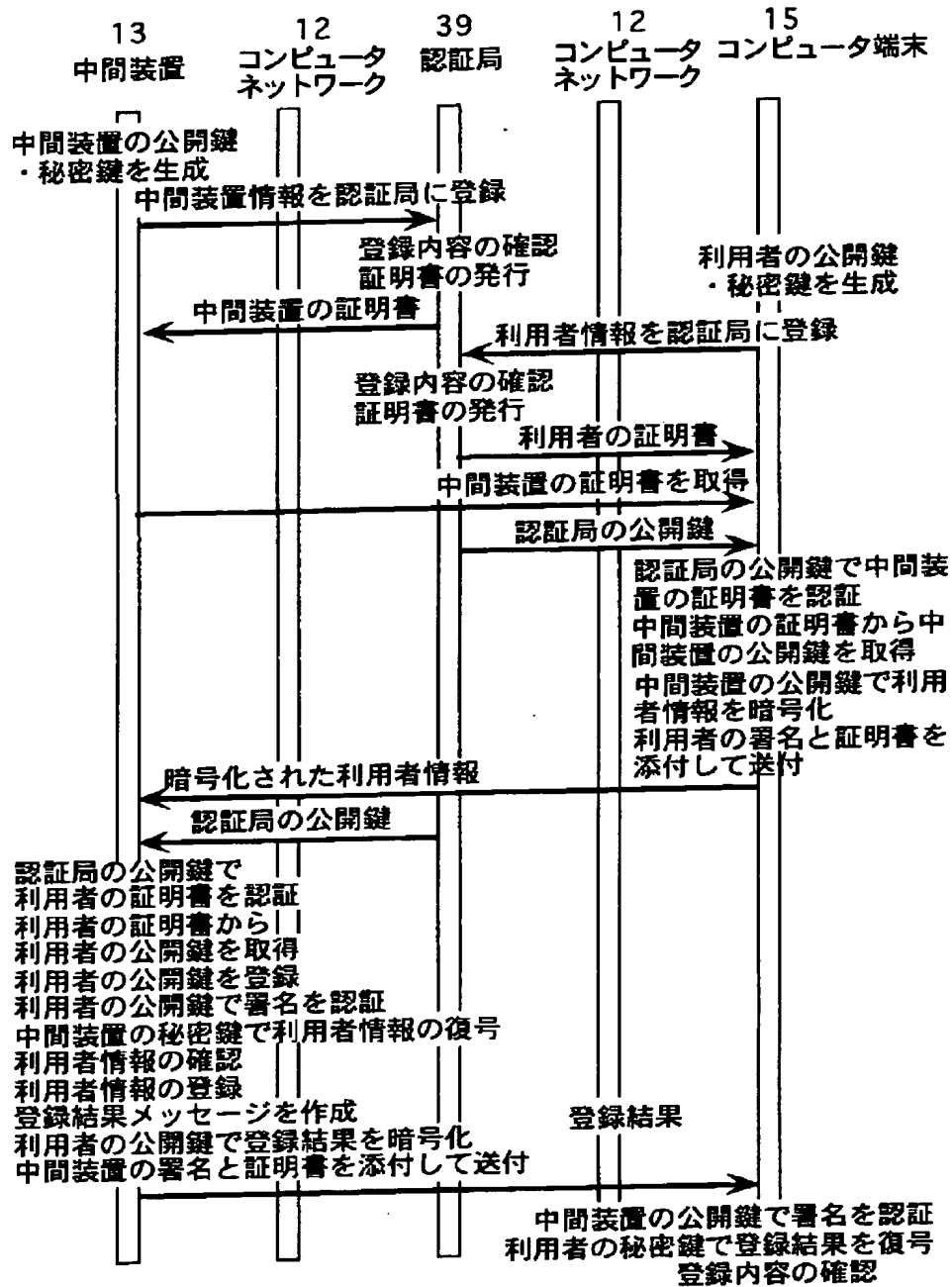


図11

フロントページの続き

(51) Int. Cl. ⁶

H 0 4 N 1/00
1/32
1/44

識別記号

1 0 7

F I

H 0 4 N 1/32

1/44

H 0 4 L 9/00

Z

6 7 5 B